5-2012

Champion Primes For Elliptic Curves

Jason Hedetniemi
Clemson University, jhedetn@clemson.edu

Champion Primes For Elliptic Curves

A Thesis
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master's
Mathematical Science

---

by
Jason T Hedetniemi
May 2012

Accepted by:
Dr. Kevin James, Committee Chair
Dr. Hui Xue, Committee Chair
Dr. Neil Calkin
Dr. James Brown

Abstract

Let $E_{a,b}$ be the elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$. A well known result of Hasse states that over $\mathbb{F}_p$

$$(p+1) - 2\sqrt{p} \leq \#E_{a,b} \leq (p+1) + 2\sqrt{p}.$$

If $\#E_{a,b} = (p+1) + \lfloor 2\sqrt{p} \rfloor$ over $\mathbb{F}_p$ and $E_{a,b}$ is nonsingular, then we call p a champion prime for $E_{a,b}$. We will discuss methods for finding champion primes for elliptic curves. In addition, we will show that the set of elliptic curves which have a champion prime has density one.

Acknowledgments

My thanks go out to my two committee chairs Dr. Kevin James and Dr. Hui Xue for their insightful guidance and invaluable help. I would also like to thank Dr. Neil Calkin and Dr. James Brown for their helpful suggestions on improving my thesis, and for being members on my committee.

Table of Contents

Title Page . . . . . **i**

Abstract . . . . . **ii**

Acknowledgments . . . . . **iii**

List of Tables . . . . . **v**

1 Prime Distribution **1**
1.1 Prime Number Theorem 4
1.2 Dirichlet's Theorem 8

2 Elliptic Curves **11**
2.1 An Introduction 11
2.2 Existence of Champion Primes 16

3 Algorithms **33**
3.1 Legendre Algorithm 33
3.2 Shanks-Mestre 41

4 Further Considerations **48**

List of Tables

1.1 Values of $\pi(x)$ 2
1.2 The Density of the Primes 3
1.3 Comparing $\pi(x)$ Versus $\frac{x}{\log(x)}$ 4
1.4 Legendre's Approximation 5
1.5 Comparing $\pi(x)$ Versus $\mathrm{Li}(x)$ 7

3.1 Example Computations 36
3.2 Finding Champion Primes, $p = 7$ 41

4.1 Counting Champion Primes 49
4.2 First Champion Primes 51

Chapter 1

Prime Distribution

Prime numbers have fascinated and entranced the minds of mathematicians for centuries. The first major result involving prime numbers belongs to Euclid, who proved that there are an infinite number of primes. His proof is so simple and elegant that it is still reproduced in textbooks today. We include it here for completeness.

Proposition 1. *There are infinitely many prime numbers.*

Proof. Suppose there are finitely many prime numbers. Denote them by $p_1, p_2, \ldots, p_n$. Let

$$X = p_1 p_2 \cdots p_n + 1.$$

Let p be a prime factor of X. From the fact that

$$X - p_1 p_2 \cdots p_n = 1$$

we can see that p cannot equal p_i for $i = 1, 2, \ldots, n$ else we would have the left-hand side divisible by p and the right-hand side not divisible by p. Thus, p must be a prime distinct from $p_1, p_2, \ldots, p_n$, a contradiction. □

With the infinitude of the primes well established, mathematicians began to inquire about the distribution of the primes. That is, how many primes are less than 100? 1,000? 10,000? 1,000,000? We make the following definition.

Definition 1. Let $\pi(x)$ denote the number of prime numbers less than or equal to x.

A table of values for $\pi(x)$ is as follows.

x	$\pi(x)$
10	4
50	15
100	25
200	46
500	95
1,000	168
2,000	303
5,000	669
10,000	1229
50,000	5133
100,000	9,592
500,000	41,538
1,000,000	78,498
5,000,000	348,513
100,000,000	5,761,455
100,000,000,000	4,118,054,813

Table 1.1: Values of $\pi(x)$

Now, we augment our table by adding a column whose values are $\pi(x)/x$.

x	$\pi(x)$	$\frac{\pi(x)}{x}$
10	4	0.4
50	15	0.3
100	25	0.25
200	46	0.23
500	95	0.19
1,000	168	0.168
2,000	303	0.152
5,000	669	0.134
10,000	1229	0.123
50,000	5133	0.103
100,000	9,592	0.096
500,000	41,538	0.083
1,000,000	78,498	0.078
5,000,000	348,513	0.070
100,000,000	5,761,455	0.058
100,000,000,000	4,118,054,813	0.0411

Table 1.2: The Density of the Primes

Thus, we can first note that the primes become less dense as x increases. We now augment our table one more time, this time adding a column whose values are $x/\log(x)$.

x	$\pi(x)$	$\frac{\pi(x)}{x}$	$\frac{x}{\log(x)}$
10	4	0.4	4.343
50	15	0.3	12.781
100	25	0.25	21.715
200	46	0.23	37.748
500	95	0.19	80.456
1,000	168	0.168	144.765
2,000	303	0.152	263.127
5,000	669	0.134	587.048
10,000	1229	0.123	1,085.736
50,000	5133	0.103	4,621.167
100,000	9,592	0.096	8,685.890
500,000	41,538	0.083	38,102.892
1,000,000	78,498	0.078	72,382.414
5,000,000	348,513	0.070	324,150.191
100,000,000	5,761,455	0.058	5,428,681.024
100,000,000,000	4,118,054,813	0.0411	3,948,131,653.666

Table 1.3: Comparing $\pi(x)$ Versus $\frac{x}{\log(x)}$

Thus, we see that $\pi(x)$ is fairly close to $\frac{x}{\log(x)}$.

1.1 Prime Number Theorem

The observation just made was first noticed by Legendre. [Gauss actually noticed this asymptotic relationship first. He, however, never published his findings.] In fact, in his

book *Essay on the Theory of Numbers* (1798) Legendre conjectured that $\pi(x) \sim \frac{x}{A \log x - B}$ where A and B were constants he would determine later. He later refined his conjecture in 1808 by specifying $A = 1$ and $B = 1.08366$. We can see that his approximation is reasonably accurate.

x	$\pi(x)$	$\frac{x}{\log(x) - 1.08366}$
10	4	8.204
50	15	17.678
100	25	28.397
200	46	47.453
500	95	97.448
1,000	168	171.701
2,000	303	306.878
5,000	669	672.628
10,000	1229	1,230.515
50,000	5133	5135.517
100,000	9,592	9588.403
500,000	41,538	41,532.712
1,000,000	78,498	78,543.178
5,000,000	348,513	348,643.709
100,000,000	5,761,455	5,768,003.712
100,000,000,000	4,118,054,813	4,124,599,868.665

Table 1.4: Legendre's Approximation

Assume for the moment that $\pi(x) \sim \frac{x}{\log(x)}$. Then, if the number of primes up to x is roughly $\frac{x}{\log(x)}$, the density of the primes up to x is $\frac{1}{\log(x)}$. Suppose we integrate this density over the

specified region. That is, take the integral

$$\int_0^x \frac{dt}{\log(t)}.$$

The result should then be a rough approximation to the number of primes up to x. However, $\frac{1}{\log(t)}$ has a singularity at $t = 1$. Thus, if we offset the limits of integration to

$$\int_2^x \frac{dt}{\log(t)}$$

we will achieve a better approximation. It was in 1849 that Chebyshev showed that such an approximation is, in fact, better than $\frac{x}{\log(x)}$. This integral is so important that it has been named the "log integral function" and is denoted by $\mathrm{Li}(x)$. That is,

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}.$$

Comparing values as before, we find the following:

x	$\pi(x)$	$\frac{x}{\log(x)}$	$\frac{x}{\log(x)-1.08366}$	$\mathrm{Li}(x)$
10	4	4.343	8.204	6.166
50	15	12.781	17.678	18.469
100	25	21.715	28.397	30.126
200	46	37.748	47.453	50.192
500	95	80.456	97.448	101.794
1,000	168	144.765	171.701	177.610
2,000	303	263.127	306.878	314.809
5,000	669	587.048	672.628	684.280
10,000	1229	1,085.736	1,230.515	1,246.137
50,000	5133	4,621.167	5135.517	5,166.547
100,000	9,592	8,685.890	9588.403	9,629.809
500,000	41,538	38,102.892	41,532.712	41,606.289
1,000,000	78,498	72,382.414	78,543.178	78,627.549
5,000,000	348,513	324,150.191	348,643.709	348,638.115
100,000,000	5,761,455	5,428,681.024	5,768,003.712	5,762,209.375
100,000,000,000	4,118,054,813	3,948,131,653.666	4,124,599,868.665	4,118,066,400.622

Table 1.5: Comparing $\pi(x)$ Versus $\mathrm{Li}(x)$

Thus, $\mathrm{Li}(x)$ appears to be a better approximation than both $\frac{x}{\log(x)}$ and Legendre's approximation $\frac{x}{\log(x)-1.08366}$.

Finally, in 1896, Hadamard and De la Vallée Poussin proved independently the Prime Number Theorem.

Theorem 2. *(Prime Number Theorem) The number of primes less than a given quantity $\pi(x)$ satisfies the following asymptotic relationship:*

$$\pi(x) \sim \frac{x}{\log x}.$$

That is,

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log(x)}} = 1.$$

In 1899, De la Vallée Poussin then confirmed that $\mathrm{Li}(x)$ is a better approximation than $\frac{x}{\log x}$ to $\pi(x)$. He proved that (see [3, p. 367])

$$\pi(x) = \mathrm{Li}(x) + O\left(\frac{x}{\log^{\alpha} x}\right) \quad \forall\, \alpha > 0.$$

The proofs of Hadamard and De la Vallée Poussin were not elementary and included deep tools from complex analysis. Many believed an elementary proof of the Prime Number Theorem could not be found until such a proof *was* found in 1949 by Selberg and Erdős which used only the simplest facts of real analysis. For a more thorough history of the prime number theorem, we encourage the reader to see [6].

1.2 Dirichlet's Theorem

It has been established that there are an infinite number of primes. One might be interested in how many primes satisfy a given modular congruence. For example, consider the arithmetic progression

$$3, 5, 7, 9, 11, 13, 15, \ldots$$

Each integer in this progression is congruent to 1 modulo 2. Are there an infinite number of primes congruent to 1 modulo 2? Of course! Since every prime $p > 2$ is odd, it must be the

case that this arithmetic progression contains an infinite number of primes. Consider now the arithmetic progression

$$2, 4, 6, 8, 10, 12, 14, \ldots$$

Here, each integer in the progression is congruent to 0 modulo 2. One can easily see that this arithmetic progression does not contain infinitely many primes since 2 is the only even prime. These examples, however, are trivial when it comes to looking for primes in an arithmetic progression. Can similar results be found for other arithmetic progressions?

A simple consideration will show that the arithmetic progression $a+bn$, $n = 0, 1, 2, \ldots$ can contain an infinite number of primes only if a and b share no common factors. That is, only if $\gcd(a, b) = 1$. Bearing this in mind, consider the following arithmetic progression

$$3, 7, 11, 15, 19, 23, 27, 31 \ldots$$

of integers congruent to 3 modulo 4. We see that in the list above, six primes were found. Does this progression have an infinite number of primes? The answer, it turns out, is yes. We prove this fact.

Proposition 3. *The arithmetic progression* $4n-1, n = 1, 2, 3, \ldots$ *contains an infinite number of primes.*

Proof. Suppose the arithmetic progression $4n - 1, n = 1, 2, 3, \ldots$ contains a finite number of primes. Let p be the largest such prime. Then define

$$N = 4(3 \cdot 5 \cdot 7 \cdot 11 \cdot \cdots \cdot p) - 1.$$

where the product (after 4) runs over all primes less than or equal to p excluding 2. We can see that $N > p$ and that N is of the form $4n - 1$. Thus, by our assumption that p is the

largest prime of the form $4n-1$, we see that N cannot be prime. We note that no prime less than or equal to p divides N, in which case all of the prime factors of N must be greater than p. Thus, all prime factors of N must be of the form $4n+1$. But the product of primes of the form $4n+1$ is also of the form $4n+1$. Thus, one prime factor of N must be of the form $4n-1$, a contradiction. □

Similar proof techniques can be used to show that other arithmetic progressions have an infinite number of primes. A general result, proven with analytic techniques, was given by Dirichlet.

Theorem 4. *(Dirichlet's Theorem) Given an arithmetic progression of terms $a \cdot n + b$ for $n = 1, 2, \ldots$ and $a > 0$, the sequence contains an infinite number of primes if and only if a and b are relatively prime.*

Asymptotic relationships similar to the Prime Number Theorem have been established for primes in arithmetic progression. For example, Siegel and Walfisz proved the following theorem.

Theorem 5. *(Siegel-Walfisz) (see [5, Theorem 1.4.6]) For any number $n > 0$ there is a positive number $C(n)$ such that for all relatively prime integers a and d with $d < \log^n x$*

$$\pi(x; d, a) = \frac{1}{\varphi(d)}\mathrm{Li}(x) + O\Big(x \exp\big(-C(n)\sqrt{\log x}\big)\Big)$$

where $\pi(x; d, a)$ denotes the number of primes less than or equal to x which are congruent to a modulo d, $\varphi(d)$ is Euler's φ-function, and the big-O constant is absolute.

Chapter 2

Elliptic Curves

2.1 An Introduction

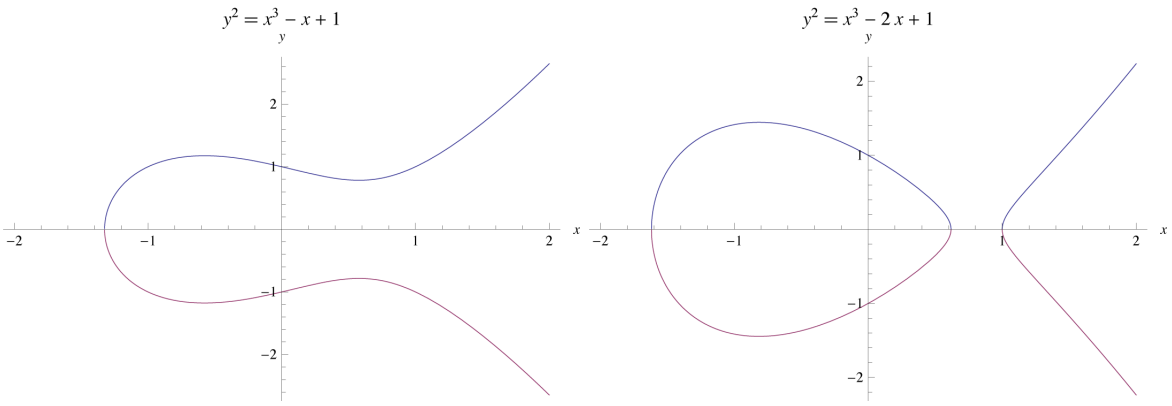
We begin our discussion of elliptic curves with the following definition.

Definition 2. A cubic curve over K is the set of solutions to an equation of the form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

where the coefficients lie in some field K.

For example, the real solutions to two sample cubic curves are given below.



Suppose we have a cubic curve E defined as above. For ease, we assume that one of a, b, c or d is nonzero so that the curve really is of degree 3. Additionally, we assume that the polynomial is absolutely irreducible over the algebraic closure of K. A pair $(x, y) \in K \times K$ that satisfies our equation is said to be an affine solution rational over K. Now, one can similarly define the curve $\tilde{E}$

$$ax^3 + bx^2y + cy^2 + dy^3 + ex^2z + fxyz + gy^2z + hxz^2 + iyz^2 + jz^3 = 0$$

whose nontrivial solutions $(x, y, z) \in K \times K \times K$ are called projective solutions. It is straightforward to check that if (x, y, z) is a solution to the polynomial above, then so is (tx, ty, tz) if $t \in K$. Thus, in some sense we consider these two solutions to be the same and say that we have one solution

$$[x, y, z] = \{(x', y', z') \, : \, x' = tx, y' = ty, z' = tz, t \in K\}$$

to the projective curve $\tilde{E}$.

If we have an affine solution (x, y) on E then $[x, y, 1]$ will be a projective solution on $\tilde{E}$. Similarly, if $[x, y, z]$ is a projective solution on $\tilde{E}$ with $z \neq 0$ then $(\frac{x}{z}, \frac{y}{z})$ will be an affine solution on E. The projective solutions $[x, y, z]$ with $z = 0$ are called points at infinity.

A projective curve is said to be nonsingular over K if over the algebraic closure of K there is no point $[x, y, z]$ where all three partial derivatives vanish. We are now in position to define an elliptic curve.

Definition 3. Let K be a field. An elliptic curve over K is a non-singular projective plane cubic curve E together with a nonzero point with coordinates in K.

It turns out that the points of an elliptic curve, together with one point at infinity, can be made into an abelian group with the point at infinity serving as the identity of the group.

By making a birational variable substitution (see [10, 1.3]), any elliptic curve can be represented by an affine equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Even nicer, if the characteristic of K is not 2 or 3, then any elliptic curve can be represented by

$$y^2 = x^3 + a_4x + a_6.$$

Either of the forms above is known as the *Weierstrass normal form.* In our work, we will focus only on elliptic curves over fields of characteristic greater than three. Thus, we will concern ourselves only with the latter form.

Given an arbitrary cubic curve, we can determine if the curve is nonsingular by considering its discriminant.

Definition 4. The discriminant of a cubic polynomial $f(x) = x^3 + ax + b$ over a field K is $-4a^3 - 27b^2$.

If the discriminant of f is zero, then the cubic curve $y^2 = f(x)$ will be singular. As mentioned above, since we are particularly interested in fields of characteristic greater than three, we make the following special definition of an elliptic curve.

Definition 5. Let p be a prime number greater than 4, and let $f(x)$ be a cubic polynomial with integer coefficients. If the discriminant of the curve is nonzero (mod p), then the set of solutions to the congruence $y^2 \equiv f(x) \,(\mathrm{mod}\, p)$ with the point at infinity is said to be an

elliptic curve over $\mathbb{F}_p$.

Since there are only finitely many elements in a finite field, we can see that the number of points on any elliptic curve over a finite field must be finite. The number of such points will be the main focus of our work to follow. We make the following definition.

Definition 6. Let $\#E_{a,b}(\mathbb{F}_p)$ denote the number of points on the elliptic curve $E_{a,b} : y^2 = x^3 + ax + b$ over $\mathbb{F}_p$.

By a famous result of Hasse, we have the following:

Theorem 6. *(Hasse). The order $\#E_{a,b}(\mathbb{F}_p)$ satisfies*

$$|\#E_{a,b}(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}.$$

In particular

$$(p+1) - 2\sqrt{p} \leq \#E_{a,b}(\mathbb{F}_p) \leq (p+1) + 2\sqrt{p}.$$

Of particular interest is the quantity a_p which we define as follows:

Definition 7. Let $a_p = p + 1 - \#E_{a,b}(\mathbb{F}_p)$.

Given our definition for a_p above, as a corollary to Hasse's theorem we have that

$$-2\sqrt{p} \leq a_p \leq 2\sqrt{p}.$$

We have finally arrived at the main focus of our work. Since a_p is always bounded below by $-2\sqrt{p}$ and above by $2\sqrt{p}$, we ask the following simple question:

Given an elliptic curve $E_{a,b}$, for what values of p does $a_p = -\lfloor 2\sqrt{p} \rfloor$?

That is, we wish to determine how often the number of points on an elliptic curve over a finite field $\mathbb{F}_p$ hits its upper bound when we vary p. We make the following definition:

Definition 8. If prime p is such that $a_p = -\lfloor 2\sqrt{p} \rfloor$ on $E_{a,b}$, with $E_{a,b}$ nonsingular over $\mathbb{F}_p$, we call p a *champion prime* for $E_{a,b}$.

Before proceeding with our work, we need to introduce a few more concepts. Consider the elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{Q}$ where A and B are integers. Let p be a prime and suppose that $p \nmid (4A^3 + 27B^2)$. If we take the equation for our curve and multiply both sides by p^6 we then have

$$p^6 y = x^3 p^6 + A p^6 x + B p^6.$$

Suppose then that we let $X = p^2 x$ and $Y = p^3 y$. Then our equation becomes

$$E' : Y^2 = X^3 + A p^4 X + B p^6$$

which is the Weierstrass form for another elliptic curve. Notice that if we have a point on E, then we will also have a point on E' and vice versa. Thus, we say that E and E' are isomorphic since their respective points are in birational correspondence. In general, elliptic curves E and E' defined over K are isomorphic over some extension L of K (possibly $L = K$) if a rational linear change of variables can turn E into E'. When the characteristic of the field K is not 2 or 3 (which is the case we are interested in) the only change of variables which preserve the form $y^2 = x^3 + Ax + B$ over K are the substitutions $x = u^2 x'$ and $y = u^3 y'$ where $u \in \overline{K}^*$ (see [9, Ch. 3 Section 1]). If E and E' are isomorphic, they are said to be two different *models* for the same elliptic curve. Thus, in referring to an elliptic curve $E : y^2 = x^3 + Ax + B$, we are really specifying a particular model for an isomorphism class of elliptic curves.

With E and E' defined as above, we see that while the discriminant of E is not divisible by p (by assumption), the discriminant of E' is. In fact, the discriminant of E' is divisible by p^{12}. Thus, we see that by considering different models for the same elliptic curve, we could potentially reduce the power of p that divides the discriminant. Thus, we say an elliptic curve E is *minimal at* p provided that the power of p dividing the discriminant of E is a minimum over the isomorphism class of E. Furthermore, an elliptic curve is said to have *good reduction at* p if its discriminant is not divisible by p. Note that if a curve has good reduction at p, then it is necessarily minimal at p as well. In general, a *minimal model* is an elliptic curve that is minimal at all primes p.

Finally, we note that if E is the elliptic curve $y^2 = x^3 + Ax + B$ over a field K, then the quadratic twist of E by a non-square $n \in K$ is the elliptic curve $E_n : ny^2 = x^3 + Ax + B$. We further note that such E and E_n will be isomorphic over $K(\sqrt{n})$.

2.2 Existence of Champion Primes

The intelligent reader may have scoffed at our definition of champion primes in that we have not yet shown that champion primes ever occur. Thus, before proceeding even further, we need to prove that champion primes do exist. This fact, however, is an easy consequence of a theorem by Deuring. To understand Deuring's theorem, we first need to consider a couple of definitions (see [2, 5.3.2]).

Definition 9. For $D < 0$, let $h(D)$ denote the number of classes of primitive positive definite quadratic forms of discriminant D, and let $w(D)$ be the number of roots of unity in the quadratic order of discriminant D.

Continuing on, we next define the Hurwitz class number.

Definition 10. For N, a non-negative integer, the Hurwitz class number $H(N)$ is defined as follows

- If $N \equiv 1$ or 2 modulo 4, then $H(N) = 0$.
- If $N = 0$ then $H(0) = -1/12$.
- Otherwise, we define $H(N)$ as the class number of not necessarily primitive (positive definite) quadratic forms of discriminant $-N$, except for forms equivalent to $a(x^2+y^2)$ which are counted with coefficient $1/2$, and those equivalent to $a(x^2 + xy + y^2)$ are counted with coefficient $1/3$.

The following proposition will be useful in our work to come.

Proposition 7. *(See [2, Lemma 5.3.7]) For $N > 0$ we have*

$$H(N) = 2 \sum_{\substack{f^2 | N \\ \frac{-N}{f^2} \equiv 0,1 \pmod 4}} \frac{h(-N/f^2)}{w(-N/f^2)}.$$

Given these definitions, we may now state the following important theorem from Deuring.

Theorem 8. *(see [4, 14.C]) Let $p > 3$ be prime, and let $N = p + 1 - a$ be an integer, where $-2\sqrt{p} \leq a \leq 2\sqrt{p}$. Then the number of non-isomorphic elliptic curves E over $\mathbb{F}_p$ which have $\#E(\mathbb{F}_p) = N = p + 1 - a$ is*

$$\frac{p-1}{2} H(4p - a^2)$$

where H is the Hurwitz class number.

As $\frac{p-1}{2} H(4p - a^2) \geq 1$ when $4p - a^2 \neq 0$, we have the following corollary:

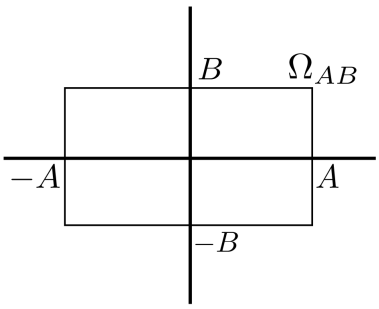
Corollary 9. *For any prime p, there exists an elliptic curve so that p is a champion prime.*

Thus, we now know that champion primes do occur. However, the alternative question is much more difficult to answer. Namely, does a given elliptic curve have a champion prime? That is, given an elliptic curve E with integer coefficients, is there a prime p so that $a_p = -\lfloor 2\sqrt{p} \rfloor$? To provide a partial answer to this question, we will consider a density argument. Namely, if we consider a box in the plane and fix some bound X, we can calculate the density of curves in this box which have a champion prime less than X. Letting our box grow will then provide a density of all curves which have a champion prime less than X. If we then let our bound X grow, we can obtain a density of curves which have a champion prime. In this manner, we will show that the density of curves which have a champion prime is 1.

We first present the notation that we will use in our work to come. A function $f(x) = O(g(x))$ if there exists a constant B such that $|f(x)| \leq Bg(x)$ for all x. Similarly, we write $f(x) \ll g(x)$ if there exist constants B and N so that $|f(x)| \leq Bg(x)$ for all $x \geq N$. We say that $f(x) = o(g(x))$ if

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0.$$

Let Ω_{AB} $(A, B > 0)$ be the box in the Cartesian plane ranging from $-A$ to A along the horizontal axis and from $-B$ to B along the vertical axis.



Throughout our work, the variable X will always satisfy $X < A, B$. We then let $N(A, B, X)$

equal the number of curves $E_{a,b}$ with $(a,b) \in \Omega_{AB}$ for which there exists a prime p, $4 < p < X$, so that $E_{a,b}$ has good reduction at p and p is a champion prime for $E_{a,b}$. Similarly, for $4 < p_1 < p_2 < \cdots < p_k < X$ we let $N_{p_1 p_2 \cdots p_k}(A,B,X)$ equal the number of curves $E_{a,b}$ with $(a,b) \in \Omega_{AB}$ which have good reduction at each p_i and have each p_i as a champion prime. By dividing by the total area of Ω_{AB}, we now naturally define

$$\delta(A,B,X) := \frac{N(A,B,X)}{4AB}$$

to be the density of curves in Ω_{AB} which have good reduction at a champion prime p, $4 < p < X$. If the limit exists, we define

$$\delta(X) := \lim_{A \to \infty} \delta(A,A,X)$$

to be the density of curves which have good reduction at a champion prime p, $4 < p < X$. Finally, if $A(X), B(X)$ are functions satisfying $A(X), B(X) \gg \exp((\frac{5}{8} + \epsilon)X)$ it is natural to define

$$\delta := \lim_{X \to \infty} \delta(A(X), B(X), X)$$

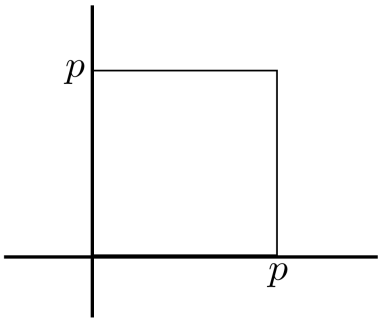
to be the density of elliptic curves which have good reduction at a champion prime. Using this notation, our first result is as follows.

Theorem 10. *Suppose A, B and $X < A, B$ are real numbers. We have the following formula for $N(A,B,X)$, the number of curves $E_{a,b}$ with $(a,b) \in \Omega_{AB}$ for which there exists a prime p, $4 < p < X$ so that $E_{a,b}$ has good reduction at p and p is a champion prime:*

$$N(A,B,X) = 4AB\left[1 - \prod_{4<p<X}\left[1 - \frac{p-1}{2p^2}H(4p - \lfloor 2\sqrt{p}\rfloor^2)\right]\right] + O\left(A\left(\exp\left(\frac{1}{4}X + o(X)\right) - 1\right)\right.$$

$$\left. + B\left(\exp\left(\frac{1}{4}X + o(X)\right) - 1\right) + \exp\left(\frac{5}{4}X + o(X)\right) - 1\right).$$

Proof. Fix a prime $4 < p < X$ where $A, B > X$. We first compute the number of integer pairs in Ω_{AB} for which the curve $E_{a,b}$ has p as a champion prime. We first consider the following region:



Deuring's Theorem implies that the number of curves in this box which have good reduction at p and have p as a champion prime is

$$\frac{p-1}{2}H(4p - \lfloor 2\sqrt{p} \rfloor^2).$$

Now, this $p \times p$ box can be translated and moved around within Ω_{AB}. In fact the number of times we can fit this box within Ω_{AB} is

$$\left(\frac{2A}{p} + \mathcal{O}(1)\right)\left(\frac{2B}{p} + \mathcal{O}(1)\right).$$

Thus, we have that

$$N_p(A, B, X) = \left(\frac{2A}{p} + \mathcal{O}(1)\right)\left(\frac{2B}{p} + \mathcal{O}(1)\right)\frac{p-1}{2}H(4p - \lfloor 2\sqrt{p} \rfloor^2).$$

We consider this expression. First, let $x = \lfloor 2\sqrt{p} \rfloor$. Then we see that

$$\begin{aligned} x \leq \sqrt{4p} \leq x+1 \quad &\Rightarrow \quad x^2 \leq 4p \leq x^2 + 2x + 1 \\ &\Rightarrow \quad 0 \leq 4p - x^2 \leq 2x + 1 \leq 4\sqrt{p} + 1. \end{aligned}$$

Thus, we see that

$$4p - \lfloor 2\sqrt{p} \rfloor^2 = \mathcal{O}(\sqrt{p}).$$

Now, for notational ease, let $\Delta_p = 4p - \lfloor 2\sqrt{p} \rfloor$. We then note that

$$\begin{aligned}
H(\Delta) &= 2 \sum_{\substack{f^2 | \Delta \\ \frac{-\Delta}{f^2} \equiv 0,1 \pmod 4}} \frac{h(-\Delta/f^2)}{w(-\Delta/f^2)} \\
&= \frac{1}{\pi} \sum_{\substack{f^2 | \Delta \\ \frac{-\Delta}{f^2} \equiv 0,1 \pmod 4}} \frac{\sqrt{\Delta}}{f} L(1, \chi_{-\Delta/f^2}) \text{ (see [2, Prop 5.3.12])} \\
&\ll \sum_{\substack{f^2 | \Delta \\ \frac{-\Delta}{f^2} \equiv 0,1 \pmod 4}} \frac{\sqrt{\Delta}}{f} \log(-\Delta) \text{ (see [1, Section 4])} \\
&\ll p^{1/4} \log(p) \sum_{\substack{f^2 | \Delta \\ \frac{-\Delta}{f^2} \equiv 0,1 \pmod 4}} \frac{1}{f} \\
&\ll p^{1/4} (\log p)^2
\end{aligned}$$

in which case

$$H(4p - \lfloor 2\sqrt{p} \rfloor^2) = \mathcal{O}(p^{1/4} (\log p)^2).$$

Using this fact, we find through expansion that

$$\begin{aligned} N_p(A,B,X) &= \left(\frac{2A}{p}+\mathcal{O}(1)\right)\left(\frac{2B}{p}+\mathcal{O}(1)\right)\frac{p-1}{2}H(4p-\lfloor 2\sqrt{p}\rfloor^2) \\ &= \frac{4AB(p-1)}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2) \\ &\quad +\left[\mathcal{O}\left(\frac{A}{p}\right)+O\left(\frac{B}{p}\right)+O(1)\right]\frac{p-1}{2}H(4p-\lfloor 2\sqrt{p}\rfloor^2) \\ &= \frac{4AB(p-1)}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)+O\left(Ap^{1/4}(\log p)^2\right) \\ &\quad +O(Bp^{1/4}(\log p)^2)+O(p^{5/4}(\log p)^2) \\ &= \frac{4AB(p-1)}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)+O\left((A+B+p)p^{1/4}(\log p)^2\right). \end{aligned}$$

Now, suppose that q is a prime distinct from p. We next consider $N_{pq}(A,B,X)$, the number of curves in Ω_{AB} which have good reduction at both p and q and have both p and q as champion primes. As seen above, there are $\frac{p-1}{2}H(4p-\lfloor 2\sqrt{p}\rfloor)$ curves which have good reduction at p and have p as a champion prime in the $p\times p$ box. Similarly, there will be $\frac{q-1}{2}H(4q-\lfloor 2\sqrt{q}\rfloor^2)$ curves which have good reduction at q and have q as a champion prime in the corresponding $q\times q$ box. Given this, the number of curves which have good reduction at p and q and have p and q as a champion prime in the $pq\times pq$ box must be

$$\frac{p-1}{2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\frac{q-1}{2}H(4q-\lfloor 2\sqrt{q}\rfloor^2).$$

This is because $H(4p-\lfloor 2\sqrt{p}\rfloor^2)$ ultimately counts the number of arithmetic progressions (A,B) modulo p such that if $(a,b)=(A,B) \pmod p$ then $E_{a,b}$ has p as a champion prime. Similarly, $H(4q-\lfloor 2\sqrt{q}\rfloor^2)$ counts the number of arithmetic progressions (A,B) modulo q such that if $(a,b)=(A,B) \pmod q$ then $E_{a,b}$ has q as a champion prime. The Chinese Remainder Theorem implies that for each respective arithmetic progression modulo p and

q, there is a unique arithmetic progression modulo pq. Thus we have that

$$N_{pq}(A,B,X) = \left(\frac{2A}{pq} + O(1)\right)\left(\frac{2B}{pq} + O(1)\right)\frac{p-1}{2}H(4p - \lfloor 2\sqrt{p}\rfloor^2)\frac{q-1}{2}H(4q - \lfloor 2\sqrt{q}\rfloor^2).$$

Our main interest, however, is in the quantity $N(A,B,X)$. By appealing to inclusion/exclusion techniques, we find that

$$\begin{aligned} N(A,B,X) &= \sum_{4<p<X} N_p(A,B,X) - \sum_{4<p<q<X} N_{pq}(A,B,X) + \sum_{4<p<q<r<X} N_{pqr}(A,B,X) \\ &\quad - \cdots + (-1)^{(\pi(X)-2)+1} N_{p_1p_2\cdots p_n}(A,B,X) \\ &= \sum_{k=1}^{\pi(X)-2} (-1)^{k+1} \sum_{\substack{n=p_1\cdots p_k \\ 4<p_i<X}} N_n(A,B,X). \end{aligned}$$

Now, we concentrate on the inner term $N_n(A,B,X)$. Let $n = p_1p_2\cdots p_k$. By applying our work above inductively, we see that

$$\begin{aligned} N_n(A,B,X) &= \left[\prod_{p|n}\frac{p-1}{2}H(4p - \lfloor 2\sqrt{p}\rfloor^2)\right]\left(\frac{2A}{n} + O(1)\right)\left(\frac{2B}{n} + O(1)\right) \\ &= \left[\prod_{p|n}\frac{p-1}{2}H(4p - \lfloor 2\sqrt{p}\rfloor^2)\right]\left(\frac{4AB}{n^2} + O\left(\frac{A}{n} + \frac{B}{n} + \frac{n}{n}\right)\right) \\ &= \frac{4AB}{n^2}\left[\prod_{p|n}\frac{p-1}{2}H(4p - \lfloor 2\sqrt{p}\rfloor^2)\right] \\ &\quad + O\left(\frac{A}{n} + \frac{B}{n} + \frac{n}{n}\right)\left[\prod_{p|n}\frac{p-1}{2}H(4p - \lfloor 2\sqrt{p}\rfloor^2)\right] \\ &= \frac{4AB}{n^2}\left[\prod_{p|n}\frac{p-1}{2}H(4p - \lfloor 2\sqrt{p}\rfloor^2)\right] + O\left(\frac{1}{2^k}(A+B+n)n^{1/4}\prod_{p|n}(\log p)^2\right). \end{aligned}$$

Thus, by substituting this into our expression for $N(A,B,X)$ we have

$$N(A,B,X) = \sum_{k=1}^{\pi(X)-2} (-1)^{k+1} \sum_{\substack{n=p_1\cdots p_k \\ 4<p_i<X}} \left[\frac{4AB}{n^2} \left[\prod_{p|n} \frac{p-1}{2} H(4p - \lfloor 2\sqrt{p} \rfloor^2) \right] + \right.$$

$$\left. O\left(\frac{1}{2^k}(A+B+n) n^{1/4} \prod_{p|n} (\log p)^2 \right) \right].$$

We consider then, the leading term of $N(A,B,X)$. This term will be

$$\begin{aligned}
& \sum_{k=1}^{\pi(X)-2} (-1)^{k+1} \sum_{\substack{n=p_1\cdots p_k \\ 4<p_i<X}} \frac{4AB}{n^2} \left[\prod_{p|n} \frac{p-1}{2} H(4p - \lfloor 2\sqrt{p} \rfloor^2) \right] \\
= & \sum_{k=1}^{\pi(X)-2} (-1)^{k+1} \sum_{\substack{n=p_1\cdots p_k \\ 4<p_i<X}} \frac{4AB}{\prod_{i=1}^{k} p_i^2} \prod_{i=1}^{k} \frac{p_i-1}{2} H(4p_i - \lfloor 2\sqrt{p_i} \rfloor^2) \\
= & 4AB \sum_{k=1}^{\pi(X)-2} (-1)^{k+1} \sum_{\substack{n=p_1\cdots p_k \\ 4<p_i<X}} \prod_{i=1}^{k} \frac{p_i-1}{2p_i^2} H(4p_i - \lfloor 2\sqrt{p_i} \rfloor^2) \\
= & 4AB \left[1 - \prod_{4<p<X} \left[1 - \frac{p-1}{2p^2} H(4p - \lfloor 2\sqrt{p} \rfloor^2) \right] \right].
\end{aligned}$$

Now, by similar logic, the remaining term of $N(A,B,X)$ will be

$$\begin{aligned}
&\sum_{k=1}^{\pi(X)-2}(-1)^{k+1}\sum_{\substack{n=p_1\cdots p_k\\4<p_i<X}}O\left(\frac{1}{2^k}(A+B+n)n^{1/4}\prod_{p|n}(\log p)^2\right)\\
=\;& O\Bigg(\sum_{k=1}^{\pi(X)-2}\sum_{\substack{n=p_1\cdots p_k\\4<p_i<X}}\frac{1}{2^k}(A+B+n)n^{1/4}\prod_{p|n}(\log p)^2\Bigg)\\
=\;& O\Bigg(A\sum_{k=1}^{\pi(X)-2}\sum_{\substack{n=p_1\cdots p_k\\4<p_i<X}}\prod_{p|n}\frac{1}{2}p^{1/4}(\log p)^2+B\sum_{k=1}^{\pi(X)-2}\sum_{\substack{n=p_1\cdots p_k\\4<p_i<X}}\prod_{p|n}\frac{1}{2}p^{1/4}(\log p)^2\\
&+\sum_{k=1}^{\pi(X)-2}\sum_{\substack{n=p_1\cdots p_k\\4<p_i<X}}\prod_{p|n}\frac{1}{2}p^{5/4}(\log p)^2\Bigg)\\
=\;& O\Bigg(A\Bigg[\prod_{4<p<X}\left[1+\frac{1}{2}p^{1/4}(\log p)^2\right]-1\Bigg]+B\Bigg[\prod_{4<p<X}\left[1+\frac{1}{2}p^{1/4}(\log p)^2\right]-1\Bigg]\\
&+\Bigg[\prod_{4<p<X}\left[1+\frac{1}{2}p^{5/4}(\log p)^2\right]-1\Bigg]\Bigg),
\end{aligned}$$

in which case we have now simplified $N(A,B,X)$ to the following equation:

$$N(A,B,X)=4AB\left[1-\prod_{4<p<X}\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right]\right]+O\Bigg(A\Bigg[\prod_{4<p<X}\left[1+\frac{1}{2}p^{1/4}(\log p)^2\right]-1\Bigg]$$

$$+B\Bigg[\prod_{4<p<X}\left[1+\frac{1}{2}p^{1/4}(\log p)^2\right]-1\Bigg]+\Bigg[\prod_{4<p<X}\left[1+\frac{1}{2}p^{5/4}(\log p)^2\right]-1\Bigg]\Bigg).$$

Now, recall that for $|x|<1$ we have

$$\log(1-x)=-\sum_{k=1}^{\infty}\frac{x^k}{k}.$$

Given this, we see that

$$\begin{aligned}
\prod_{4<p<X}\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right] &= \exp\left(\log\left(\prod_{4<p<X}\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right]\right)\right)\\
&= \exp\left(\sum_{4<p<X}\log\left(\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right]\right)\right)\\
&= \exp\left(-\sum_{4<p<X}\sum_{k=1}^{\infty}\frac{(\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2))^k}{k}\right)\\
&= \exp\left(-\sum_{4<p<X}\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right.\\
&\quad \left.-\sum_{4<p<X}\sum_{k=2}^{\infty}\frac{(\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2))^k}{k}\right).
\end{aligned}$$

Now

$$\begin{aligned}
\sum_{4<p<X}\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2) &\gg \sum_{4<p<X}\frac{p-1}{2p^2}\\
&\gg \sum_{4<p<X}\frac{1}{p}\\
&= \log(\log(X))+O\left(\frac{1}{(\log X)^2}\right).
\end{aligned}$$

Additionally,

$$\begin{aligned}
\sum_{4<p<X}\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2) &\ll \sum_{4<p<X}\frac{p-1}{2p^2}\cdot p^{1/4}\\
&\ll \sum_{4<p<X}\frac{1}{p^{3/4}}.
\end{aligned}$$

If we let

$$a_n = \begin{cases} 1 & \text{if } n \text{ is prime,} \\ 0 & \text{otherwise,} \end{cases}$$

and $f(t) = t^{-3/4}$, then by partial summation (see [8, Theorem 2.1.1]) we find that

$$\begin{aligned} \sum_{4<p<X} \frac{1}{p^{3/4}} &= \sum_{n<X} a_n f(n) \\ &= \frac{X}{\log(X)} X^{-3/4} + \frac{3}{4} \int_2^X \frac{t^{-3/4}}{\log(t)}\, dt \\ &= \frac{X^{1/4}}{\log(X)} + \frac{3t^{1/4}}{\log(t)}\bigg|_2^X + O\left(\frac{X^{1/4}}{(\log X)^2}\right) \\ &= \frac{4X^{1/4}}{\log X} + O\left(\frac{X^{1/4}}{(\log X)^2}\right). \end{aligned}$$

Additionally,

$$\begin{aligned} \sum_{4<p<X} \sum_{k=2}^{\infty} \frac{(\frac{p-1}{2p^2} H(4p - \lfloor 2\sqrt{p} \rfloor^2)^k}{k} &= \sum_{4<p<X} \sum_{k=2}^{\infty} \frac{(p-1)^k}{2^k k p^{2k}} H(4p - \lfloor 2\sqrt{p} \rfloor^2)^k \\ &\ll \sum_{4<p<X} \sum_{k=2}^{\infty} \frac{(p-1)^k}{2^k k p^{2k}} (p^{5k/16}) \\ &\leq \sum_{4<p<X} \sum_{k=2}^{\infty} \frac{1}{(2p^{11/16})^k} \\ &= \sum_{4<p<X} \frac{1}{(2p^{11/16})^2} \cdot \frac{1}{1 - \left(\frac{1}{2p^{11/16}}\right)} \\ &= \sum_{4<p<X} \frac{1}{4p^{22/16} - 2p^{11/16}} \\ &\ll \sum_{4<p<X} \frac{1}{p^{22/16}} \\ &\ll \sum_{n \leq X} \frac{1}{n^{22/16}}. \end{aligned}$$

We note that this final sum converges as $X \to \infty$. For our fixed X, however, we now have

that

$$\exp\left(-\frac{X^{1/4}}{\log X}+O\left(\frac{X^{1/4}}{(\log X)^2}\right)+O(1)\right)\leq\prod_{4<p<X}\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right]$$

$$\leq\exp\left(-\log(\log(X))+O\left(\frac{1}{(\log X)^2}\right)+O(1)\right).$$

Moving on to the other terms in our equation for $N(A,B,X)$, we note that

$$\log(1+x)=\log(x)+O\left(\frac{1}{x}\right).$$

Using this fact, we see that

$$\begin{aligned}
\prod_{4<p<X}\left[1+\frac{1}{2}p^{1/4}\log(p)^2\right] &= \exp\left(\log\left(\prod_{4<p<X}\left[1+\frac{1}{2}p^{1/4}\log(p)^2\right]\right)\right)\\
&= \exp\left(\sum_{4<p<X}\log\left(1+\frac{1}{2}p^{1/4}\log(p)^2\right)\right)\\
&= \exp\left(\sum_{4<p<X}\left(\log\left(\frac{1}{2}p^{1/4}\log(p)^2\right)+O\left(\frac{2}{p^{1/4}\log(p)^2}\right)\right)\right)\\
&= \exp\left(\sum_{4<p<X}\left(\frac{1}{4}\log(p)+2\log(\log(p))-\log(2)+\right.\right.\\
&\quad \left.\left.O\left(\frac{2}{p^{1/4}\log(p)^2}\right)\right)\right)\\
&= \exp\left(\frac{1}{4}\sum_{4<p<X}\log(p)+2\sum_{4<p<X}\log(\log(p))-\sum_{4<p<X}\log(2)\right.\\
&\quad \left.+\sum_{4<p<X}O\left(\frac{2}{p^{1/4}\log(p)^2}\right)\right).
\end{aligned}$$

Now, we note that by the Prime Number Theorem

$$\frac{1}{4}\sum_{4<p<X}\log(p)=\frac{1}{4}X+o(X)\quad\text{and}\quad\sum_{4<p<X}O(\log\log p)=O\left(\frac{X}{\log X}\log\log X\right),$$

in which case

$$\prod_{4<p<X}\left[1+\frac{1}{2}p^{1/4}(\log p)^2\right]=\exp\left(\frac{1}{4}X+o(X)\right).$$

By the same logic, we have

$$\prod_{4<p<X}\left[1+\frac{1}{2}p^{5/4}(\log p)^2\right]=\exp\left(\frac{5}{4}X+o(X)\right).$$

Putting all of our results together, we find that

$$N(A,B,X)=4AB\left[1-\prod_{4<p<X}\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right]\right]+O\Bigg(A\left(\exp\left(\frac{1}{4}X+o(X)\right)-1\right)$$

$$+B\left(\exp\left(\frac{1}{4}X+o(X)\right)-1\right)+\exp\left(\frac{5}{4}X+o(X)\right)-1\Bigg)$$

which concludes the proof of Theorem 9. □

This result is actually quite useful in that as a consequence, we have the following corollary.

Corollary 11. *If $A(X)$ and $B(X)$ are chosen so that they satisfy*

- $A(X)\gg\exp\left(\left(\frac{1}{4}+\epsilon_1\right)X\right)$
- $B(X)\gg\exp\left(\left(\frac{1}{4}+\epsilon_2\right)X\right)$
- $A(X)B(X)\gg\exp\left(\left(\frac{5}{4}+\epsilon_3\right)X\right)$

then

$$N(A,B,X)=4A(X)B(X)\left[1-\prod_{4<p<X}\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right]\right]+o(A(X)B(X))$$

and

$$\delta(A(X), B(X), X) = \left[1 - \prod_{4<p<X} \left[1 - \frac{p-1}{2p^2} H(4p - \lfloor 2\sqrt{p} \rfloor^2)\right]\right] + o(1).$$

Furthermore, $\delta(A(X), B(X), X)$ equals the density of curves $E_{a,b}$ for which there exists a prime $4 < p < X$ such that $E_{a,b}$ has good reduction at p and has p as a champion prime.

Proof. Suppose $A(X)$ and $B(X)$ are chosen so that the above conditions hold. Then we see that

$$\lim_{X\to\infty} \frac{A(X)\left(\exp\left(\frac{1}{4}X + o(X)\right) - 1\right)}{A(X)B(X)} = 0$$

in which case

$$A(X)\left(\exp\left(\frac{1}{4}X + o(X)\right) - 1\right) = o(A(X)B(X)).$$

The same logic will then show that

$$B(X)\left(\exp\left(\frac{1}{4}X + o(X)\right) - 1\right) = o(A(X)B(X))$$

and that

$$\exp\left(\frac{5}{4}X + o(X)\right) - 1 = o(A(X)B(X)).$$

Given this, the corollary easily follows from Theorem 9. □

This corollary leads to a very nice result. Namely, if we fix a box, centered at the origin, in the plane, we can now obtain the density of curves in that box which will have a champion prime less than a determined bound.

Corollary 12. *Suppose A and B are fixed positive real numbers, and let*

$$s = \left(\frac{8}{5} - \epsilon\right)\log(\min\{A, B\})$$

Then the density of curves $E_{a,b}$ with $|a| \leq A$, $|b| \leq B$ for which there exists a prime $4 < p < s$

such that $E_{a,b}$ has good reduction at p and p is a champion prime is given by

$$\left[1-\prod_{4<p<s}\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right]\right]+o(1).$$

Proof. Immediate from Corollary 10. □

Theorem 9 also allows us to obtain our main density result.

Corollary 13. *Suppose $A(X)$ and $B(X)$ are chosen so that they satisfy the conditions of Corollary 10. Then the density of curves which have good reduction at a prime p and have p as a champion prime satisfies*

$$\delta=\lim_{X\to\infty}\delta(A(X),B(X),X)=1.$$

Proof. In the proof of Theorem 9 we proved that

$$\left[1-\prod_{4<p<X}\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right]\right]\geq 1-\exp\left(-\log\log(X)+O\left(\frac{1}{(\log X)^2}\right)+O(1)\right)$$

and that

$$\left[1-\prod_{4<p<X}\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right]\right]\leq 1-\exp\left(-\frac{X^{1/4}}{\log X}+O\left(\frac{X^{1/4}}{(\log X)^2}\right)+O(1)\right).$$

Given this, and Corollary 10, we now see that

$$\delta=\lim_{X\to\infty}\delta(A(X),B(X),X)=1$$

which concludes the proof of Corollary 12. □

We note that our density δ above is the density of curves which have good reduction at champion prime p. It is possible that an elliptic curve is non-minimal at p, but has p

as a champion prime. Thus, the number of curves which have a champion prime is strictly greater than the number of curves which have good reduction at a champion prime. In any event, since we showed that the density of curves which have good reduction at a champion p is 1, it certainly must also be the case that the density of curves which have a champion prime p is 1 as well.

Chapter 3

Algorithms

We now turn our attention to finding champion primes. Since champion primes are determined by the number of points on an elliptic curve, we must develop techniques which will allow us to count the number of points on a curve. In particular, we must develop techniques to calculate a_p for a given elliptic curve.

3.1 Legendre Algorithm

Computing the number of points on a given elliptic curve mod p can be achieved in a relatively straightforward manner. To illustrate this technique, we first recall some definitions.

Definition 11. Let p be an odd prime. Then $a \in \mathbb{F}_p$ is called a quadratic residue (modulo p) if there exists some nonzero x such that $a \equiv x^2 \pmod{p}$ and $a \not\equiv 0 \pmod{p}$. If no such x exists, then a is called a quadratic nonresidue (modulo p).

Related to quadratic residues and nonresidues is the Legendre symbol, defined as follows:

Definition 12. For p an odd prime, the Legendre symbol $(\frac{a}{p})$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

For use later, we state some properties of the Legendre symbol.

Proposition 14. *For p an odd prime*

- $(\frac{1}{p}) = 1$
- $(\frac{a^2}{p}) = 1$ *if* $p \nmid a$.
- $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.
- *If* $a \equiv b \pmod{p}$ *then* $(\frac{a}{p}) = (\frac{b}{p})$.

Consider the elliptic curve $y^2 = f(x)$ where $f(x) = x^3 + ax + b$ defined over $\mathbb{F}_p$. As defined above, the set of points on this curve is the set of solutions to the quadratic congruence $y^2 \equiv f(x) \pmod{p}$ plus the point at infinity. Let $x_0 \in \mathbb{F}_p$ and consider the quantity $f(x_0)$. If $f(x_0) \equiv 0 \pmod{p}$, then clearly the point $(x_0, 0)$ satisfies the congruence. Thus, $(x_0, 0)$ will be a point on the curve. If $f(x_0) \not\equiv 0 \pmod{p}$, then the question becomes whether there exists a $y_0 \in \mathbb{F}_p$ such that $y_0^2 \equiv f(x_0) \pmod{p}$. We recognize this condition as whether or not $f(x_0)$ is a quadratic residue mod p. If $f(x_0)$ is a quadratic residue, then there will exist a $y_0 \in \mathbb{F}_p$ such that $y_0^2 \equiv f(x_0) \pmod{p}$ in which case the points (x_0, y_0) and $(x_0, -y_0)$ will be on the curve. If $f(x_0)$ is a quadratic nonresidue mod p, then no such y_0 exists, in which case there will be no points of the form (x_0, y_0) on the curve.

Thus, to count the number of points on the curve, we simply appeal to Legendre symbols. That is, the number of points corresponding to $x_0 \in \mathbb{F}_p$ will be

$$1 + \left(\frac{f(x_0)}{p}\right) = \begin{cases} 0 & \text{if } f(x_0) \text{ is a quadratic nonresidue modulo } p \\ 1 & \text{if } f(x_0) \equiv 0 \,(\mathrm{mod}\, p), \\ 2 & \text{if } f(x_0) \text{ is a quadratic residue modulo } p \end{cases} .$$

So, to count the total number of points on the curve, we simply sum the above quantity over all $x_0 \in \mathbb{F}_p$ and include the point at infinity. Thus, we find

$$\begin{aligned} \#E_{a,b}(\mathbb{F}_p) &= 1 + \sum_{i=0}^{p-1} \left(1 + \left(\frac{f(i)}{p}\right)\right) \quad \text{(where the first 1 counts the point at infinity)} \\ &= (p+1) + \sum_{i=0}^{p-1} \left(\frac{f(i)}{p}\right). \end{aligned}$$

Now, since $\#E_{a,b}(\mathbb{F}_p) = (p+1) - a_p$, we can see that

$$a_p = -\sum_{i=0}^{p-1} \left(\frac{f(i)}{p}\right).$$

To illustrate this method for computing a_p, consider the curve $y^2 = f(x)$ where $f(x) = x^3 + 3x + 1$ over $\mathbb{F}_7$. For each $x \in \mathbb{F}_7$ we compute $f(x)$, and determine if this quantity is a quadratic residue or nonresidue modulo 7.

x	$f(x) \pmod 7$	$(\frac{f(x)}{7})$	$1 + (\frac{f(x)}{7})$	Points On Curve
0	1	1	2	$(0,1)$ and $(0,6)$
1	5	-1	0	None
2	1	1	2	$(2,1)$ and $(2,6)$
3	2	1	2	$(3,3)$ and $(3,4)$
4	0	0	1	$(4,0)$
5	1	1	2	$(5,1)$ and $(5,6)$
6	4	1	2	$(6,2)$ and $(6,5)$

Table 3.1: Example Computations

Thus, given our 11 points found, plus the point at infinity, we can see that $\#E_{3,1}(\mathbb{F}_7) = 12$. Thus, solving for a_p we find that

$$a_p = 8 - 12 = -4.$$

We note that $-\lfloor 2\sqrt{7} \rfloor = -5$ in which case 7 is not a champion prime for this curve.

3.1.1 Implementations

In order to implement the Legendre algorithm for computing the order of an elliptic curve, we must first implement code that will compute Legendre symbols. To do this, we first need to extend the definition of the Legendre Symbol.

Definition 13. The Kronecker symbol $(\frac{a}{b})$ for any $a, b \in \mathbb{Z}$ is defined as follows.

1. If $b = 0$, then $(\frac{a}{0}) = 1$ if $a = \pm 1$, and is equal to 0 otherwise.

2. If $b \neq 0$, write $b = \prod p$ where the p are not necessarily distinct primes (including

$p = 2$), or $p = -1$ to take care of the sign. Then we set

$$\left(\frac{a}{b}\right) = \prod \left(\frac{a}{p}\right),$$

where $(\frac{a}{p})$ is the Legendre symbol defined for $p > 2$, and where we define

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } a \text{ is even} \\ (-1)^{(a^2-1)/8} & \text{if } a \text{ is odd} \end{cases}$$

and

$$\left(\frac{a}{-1}\right) = \begin{cases} 1 & \text{if } a \geq 0 \\ -1 & \text{if } a < 0 \end{cases}.$$

The Kronecker symbol will agree with all Legendre symbols if b is an odd prime. To compute Kronecker symbols, we follow an algorithm analogous to the Euclidean algorithm (see for example [2, Alg 1.4.10]).

Kronecker Symbol Algorithm : Given $a, b \in \mathbb{Z}$, the following algorithm computes the Kronecker symbol $(\frac{a}{b})$.

1. If $b = 0$, then output 0 if $|a| \neq 1$, and output 1 if $|a| = 1$ and terminate the algorithm.

2. If a and b are both even, output 0 and terminate the algorithm. Otherwise, set $v \leftarrow 0$ and while b is even, set $v \leftarrow v+1$ and $b \leftarrow b/2$. Then, if v is even, set $k \leftarrow 1$, otherwise set $k \leftarrow (-1)^{(a^2-1)/8}$ (by table lookup, not computation). Finally, if $b < 0$, set $b \leftarrow -b$. If, in addition, $a < 0$, set $k \leftarrow -k$.

3. If $a = 0$, then output 0 if $b > 1$, k if $b = 1$, and terminate the algorithm. Otherwise, set $v \leftarrow 0$ and while a is even, set $v \leftarrow v+1$ and $a \leftarrow a/2$. If v is odd, set $k \leftarrow (-1)^{(b^2-1)/8}k$.

4. Set

$$k \leftarrow (-1)^{(a-1)(b-1)/4} k,$$

(using if statements and no multiplications), and then $r \leftarrow |a|$, $a \leftarrow b \bmod r$, $b \leftarrow r$ and go to step 3.

Using this Legendre symbol implementation, we can execute the Legendre algorithm.

Legendre Algorithm : Given an elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$ the following algorithm computes a_p.

1. Set $s \leftarrow 0$.
2. For $j = 0$ to $p - 1$, let $l = j^3 + Aj + B$ (reducing mod p with each step). Then, let $s \leftarrow s + (\frac{l}{p})$.
3. Output $-s$.

3.1.2 Applications

Using this algorithm alone, we can note a few simple results.

Proposition 15. *Let E be an elliptic curve of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Then 5 will be a champion prime for E if and only if $A \equiv 3 \pmod 5$ and $B \equiv 0 \pmod 5$.*

Proof. Let E be an elliptic curve of the form $y^2 = x^3 + Ax + B$, and suppose that 5 is a champion prime. Then $a_5 = -\lfloor 2\sqrt{5} \rfloor = -4$. We first note that

$$\left(\frac{0}{5}\right) = 0, \quad \left(\frac{1}{5}\right) = 1, \quad \left(\frac{2}{5}\right) = -1, \quad \left(\frac{3}{5}\right) = -1, \quad \left(\frac{4}{5}\right) = 1.$$

We next note that

$$\begin{aligned} a_5 &= -\sum_{i=0}^{4}\left(\frac{i^3+Ai+B}{5}\right) \\ &= -\Big[\left(\frac{B}{5}\right)+\left(\frac{1+A+B}{5}\right)+\left(\frac{3+2A+B}{5}\right)+\left(\frac{2+3A+B}{5}\right)+\left(\frac{4+4A+B}{5}\right)\Big]. \end{aligned}$$

Now, since $a_5 = -4$, we can see that no Legendre symbol computed in the bracketed region can equal -1. This immediately implies that $B \not\equiv 2 \pmod 5$ and $B \not\equiv 3 \pmod 5$. This leaves just three cases.

- Suppose $B \equiv 0 \pmod 5$. Then we have

$$\begin{aligned} a_5 &= -\left[0+\left(\frac{1+A}{5}\right)+\left(\frac{3+2A}{5}\right)+\left(\frac{2+3A}{5}\right)+\left(\frac{4+4A}{5}\right)\right] \\ &= -\left[\left(\frac{1+A}{5}\right)+\left(\frac{2(4+A)}{5}\right)+\left(\frac{3(4+A)}{5}\right)+\left(\frac{4(1+A)}{5}\right)\right] \\ &= -\left[\left(\frac{1+A}{5}\right)+\left(\frac{2}{5}\right)\left(\frac{4+A}{5}\right)+\left(\frac{3}{5}\right)\left(\frac{4+A}{5}\right)+\left(\frac{4}{5}\right)\left(\frac{1+A}{5}\right)\right] \\ &= -\left[2\left(\frac{1+A}{5}\right)-2\left(\frac{4+A}{5}\right)\right]. \end{aligned}$$

  Now, our assumption is that $a_5 = -4$. Thus, it must be the case that $(\frac{1+A}{5}) = 1$ and $(\frac{4+A}{5}) = -1$. By enumeration, we can see this implies that $A \equiv 3 \pmod 5$.

- Suppose $B \equiv 1 \pmod 5$. Then we have

$$\begin{aligned} a_5 &= -\left[1+\left(\frac{2+A}{5}\right)+\left(\frac{4+2A}{5}\right)+\left(\frac{3+3A}{5}\right)+\left(\frac{4A}{5}\right)\right] \\ &= -\left[1+\left(\frac{2+A}{5}\right)+\left(\frac{2(2+A)}{5}\right)+\left(\frac{3(1+A)}{5}\right)+\left(\frac{A}{5}\right)\right] \\ &= -\left[1+\left(\frac{2+A}{5}\right)+\left(\frac{2}{5}\right)\left(\frac{2+A}{5}\right)+\left(\frac{3}{5}\right)\left(\frac{1+A}{5}\right)+\left(\frac{A}{5}\right)\right] \\ &= -\left[1-\left(\frac{1+A}{5}\right)+\left(\frac{A}{5}\right)\right]. \end{aligned}$$

But we can clearly see that this will never equal -4. Thus, we have a contradiction. If $B \equiv 1 \pmod 5$ then $a_5 \neq -4$.

- Suppose $B \equiv 4 \pmod 5$. Then we have

$$\begin{aligned} a_5 &= -\left[1 + \left(\frac{A}{5}\right) + \left(\frac{2+2A}{5}\right) + \left(\frac{1+3A}{5}\right) + \left(\frac{3+4A}{5}\right)\right] \\ &= -\left[1 + \left(\frac{A}{5}\right) - \left(\frac{1+A}{5}\right) - \left(\frac{2+A}{5}\right) + \left(\frac{2+A}{5}\right)\right] \\ &= -\left[1 + \left(\frac{A}{5}\right) - \left(\frac{1+A}{5}\right)\right]. \end{aligned}$$

But this can clearly never equal -4. Thus, we have a contradiction. If $B \equiv 4 \pmod 5$, then $a_5 \neq -4$.

Thus, if $B \equiv 0 \pmod 5$ and $A \equiv 3 \pmod 5$, then $a_5 = -4$ and 5 will be a champion prime for E. Furthermore, given the above calculations, the reverse implication is clear. □

As demonstrated above, the Legendre Algorithm can be used to determine if a prime $p \geq 5$ is a champion prime for a given elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$. Moreover, this algorithm can also be used to determine values of A and B which will ensure that p is a champion prime. Notice, however, that over $\mathbb{F}_p$, there are only p possible choices for A and p possible choices for B. Ignoring the case $A = 0$ when $B = 0$ (which would create a singular curve), we see that there are $p^2 - 1$ possible elliptic curves over $\mathbb{F}_p$. Thus, using the Legendre Algorithm, we can iterate through all possible curves over $\mathbb{F}_p$ and determine for which curves p is a champion prime.

For example, when $p = 7$, there are 48 possible curves to consider. We compute a_7 for each curve:

(A,B)	a_7	(A,B)	a_7	(A,B)	a_7	(A,B)	a_7	(A,B)	a_7	(A,B)	a_7	(A,B)	a_7
(0,0)	S	(0,1)	-4	(0,2)	-1	(0,3)	-5	(0,4)	5	(0,5)	1	(0,6)	4
(1,0)	0	(1,1)	3	(1,2)	S	(1,3)	2	(1,4)	-2	(1,5)	S	(1,6)	-3
(2,0)	0	(2,1)	3	(2,2)	S	(2,3)	2	(2,4)	-2	(2,5)	S	(2,6)	-3
(3,0)	0	(3,1)	-4	(3,2)	-1	(3,3)	2	(3,4)	-2	(3,5)	1	(3,6)	4
(4,0)	0	(4,1)	3	(4,2)	S	(4,3)	2	(4,4)	-2	(4,5)	S	(4,6)	-3
(5,0)	0	(5,1)	-4	(5,2)	-1	(5,3)	2	(5,4)	-2	(5,5)	1	(5,6)	4
(6,0)	0	(6,1)	-4	(6,2)	-1	(6,3)	2	(6,4)	-2	(6,5)	1	(6,6)	4

Table 3.2: Finding Champion Primes, $p = 7$

We note that the a_7 values of "S" indicate that the curves have discriminant congruent to 0 modulo 7. Since $\lfloor 2\sqrt{7} \rfloor = 5$, we can see that over $\mathbb{F}_7$, there is only one set of curves for which 7 is a champion prime, namely those curves for which $A \equiv 0 \pmod 7$ and $B \equiv 3 \pmod 7$.

3.2 Shanks-Mestre

The Legendre Algorithm method for computing the number of points on an elliptic curve is guaranteed to always work. However, the algorithm runs in $O(p \log p)$ time. Thus, the method should only be used for primes less than, say, 1000. Furthermore, upon closer inspection, we see that the algorithm does not take advantage of the group structure on the curve. The method of Mestre and Shanks takes advantage of the group structure on the curve, producing an algorithm which runs in $O(p^{1/4+\epsilon})$ time. To understand this method, we must first consider Shank's Baby Step Giant Step Method for computing the order of a point.

3.2.1 Shank's Baby Step Giant Step Method

Suppose that G is a group, and that g is an element of G. Recall that the order of g is the smallest positive integer n such that $g^n = 1$, where by 1 we are denoting the identity element of the group. Calculating the order of g appears to be relatively straightforward. Simply compute $g, g^2, g^3, \ldots$ until the proper n is found. This, however, will take $O(n)$ group operations. If an upper bound on the order of g is known, however, a much faster algorithm can be put into effect.

Suppose B is an upper bound on the order of g. Let $q = \lceil \sqrt{B} \rceil$. Then, let

$$X = \{1, g, g^2, \ldots, g^{q-1}\}$$

and set $g_1 = g^{-q}$. We can factor the order n of g as

$$n = aq + r \quad \text{with} \quad 0 \leq r < q.$$

But note that by our choice of q, we must also have that $a \leq q$. Thus, for $a = 1, 2, \ldots, q$, compute g_1^a. If g_1^a is an element of X, then we must have

$$g_1^a = g^j \quad \text{for some } j \in \{0, 1, \ldots, q-1\}$$

in which case

$$g^{-aq} = g^j \quad \Rightarrow \quad 1 = g^{aq+j}.$$

That is, the order of g must be a divisor of $aq + j$. From there, we can factor $aq + j$ and deduce the correct order of g.

Note that in executing this algorithm, we could potentially perform q searches through our set X. If these searches are done naïvely, this will take $O(q^2)$ comparisons. However, the set X can first be sorted using an $O(q \log q)$ method. Then, a search of the sorted X will take only $O(\log q)$ comparisons, which will reduce the total computation time down to $O(q \log q)$. For more on the Baby Step Gian Step Method, we encourage the reader to see [2, 5.4.1].

3.2.2 Shanks-Mestre Algorithm

Since the points on an elliptic curve form an abelian group, we may apply Shank's Baby Step Giant Step method in order to compute the order of any point. However, our interest is in the total number of points, which is the order of the group. Recall that by Hasse's Theorem, we know that

$$(p+1) - 2\sqrt{p} \leq \#E_{a,b}(\mathbb{F}_p) \leq (p+1) + 2\sqrt{p}.$$

In addition, by Lagrange's Theorem, the order of any point must divide the order of the group. Thus, given any point P on $E_{a,b}$ of order n, there must be at least one multiple of n that lies within the Hasse interval. Notice that the length of the Hasse interval is $4\sqrt{p}$. Thus, if we have a point P on our elliptic curve and we find the order of P (using the Baby Step Giant Step method) to be $n > 4\sqrt{p}$, then there must be *only one* multiple of n which lies within the Hasse interval. Moreover, this multiple must be the order of the curve itself. Thus, in order to find the number of points on an elliptic curve, it suffices to find a point of sufficient order, and then find the multiple of its order which lies within the Hasse interval.

Unfortunately, it is possible that all points on a given elliptic curve have small order. That is, we may not be able to find a point whose order is greater than $4\sqrt{p}$. Thanks to a

result by Mestre, we can avoid this pitfall.

Theorem 16. *(see [5, Theorem 7.5.2]) For an elliptic curve $E_{a,b}$ over $\mathbb{F}_p$ and its twist $E'_{A,B}$ over $\mathbb{F}_p$ by a quadratic nonresidue mod p we have that*

$$\#E_{a,b}(\mathbb{F}_p) + \#E'_{A,B}(\mathbb{F}_p) = 2p + 2.$$

When $p > 457$, there exists a point of order greater than $4\sqrt{p}$ on at least one of the two elliptic curves, $E_{a,b}, E'_{A,B}$. Furthermore, if $p > 229$, at least one of the two curves possesses a point P with order n for which the only multiple of n in the Hasse interval is the actual curve order.

A key point is that if we know the number of points on the quadratic twist $E'_{A,B}$, we can deduce the number of points on $E_{A,B}$ by the relation $\#E_{A,B}(\mathbb{F}_p) + \#E'_{A,B}(\mathbb{F}_p) = 2p + 2$. Given this, we can now appeal to the Shanks-Mestre Algorithm. Find a point P on $E_{A,B}$. Use the Baby Step Giant Step method to compute the order of P. If the order of P is greater than $4\sqrt{p}$, deduce the order of the original elliptic curve $E_{A,B}$. If the order of P is less than $4\sqrt{p}$, find a point Q on $E'_{A,B}$. Use the Baby Step Giant Step method to compute the order of Q. If the order of Q is greater than $4\sqrt{p}$, deduce the order of the quadratic twist $E'_{A,B}$ and thus the order of $E_{A,B}$. If the order of Q is less than $4\sqrt{p}$, begin again. Thanks to the result of Mestre, we are guaranteed that this algorithm will terminate if $p > 457$.

3.2.3 Shanks-Mestre Implementation

The Shanks-Mestre algorithm is noticeably more involved than the Legendre algorithm. In particular, the Shanks-Mestre algorithm incorporates the group structure of the elliptic curve. Thus, in order to implement the Shanks-Mestre algorithm, we must first implement code that will perform the necessary group operations on an elliptic curve. That is, we must implement code that will add two points on an elliptic curve and code that will

raise a point to a power.

We first consider adding two points on an elliptic curve. We modify a Mathematica implementation set forth by Erickson and Vazzana (see [7, 11.9 Notes]).

Elliptic Curve Addition : Given two points $P_1 = (x_1, y_1, z_1), P_2 = (x_2, y_2, z_2)$ (written in projective coordinates) on the elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$, we compute the sum $P_1 + P_2$.

1. If $z_1 = 0$ (i.e. if P_1 is the point at infinity), return (x_2, y_2, z_2).

2. If $z_2 = 0$ (i.e. if P_2 is the point at infinity), return (x_1, y_1, z_1).

3. If $x_1 \equiv x_2 \pmod{p}$ and $y_1 \equiv -y_2 \pmod{p}$ return $(0, 1, 0)$ (the point at infinity).

4. If $x_1 \equiv x_2 \pmod{p}$ and $y_1 \not\equiv -y_2 \pmod{p}$ set $x_3 \leftarrow \left(\frac{3x_1^2+A}{2y_1}\right)^2 - 2x_1$, $y_3 \leftarrow -\left(\frac{3x_1^2+A}{2y_1}\right)(x_3 - x_1) + y_1$ and $z_3 \leftarrow 1$ where all computations are done modulo p and division by $2y_1$ corresponds to multiplying by the multiplicative inverse of $2y_1$ modulo p. Return (x_3, y_3, z_3).

5. If $x_1 \not\equiv x_2 \pmod{p}$, set $x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2$, $y_3 \leftarrow -\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_3 - x_1) + y_1$, $z_3 \leftarrow 1$ where, once again, all computations are done modulo p and division by $x_2 - x_1$ corresponds to multiplication by the multiplicative inverse of $x_2 - x_1$ modulo p. Return (x_3, y_3, z_3).

We next consider elliptic curve multiplication. Once again, we adapt a Mathematica implementation set forth by Erickson and Vazzana (see [7, 11.9 Notes]).

Elliptic Curve Multiplication: Given a point $P = (x, y, z)$ (written in projective coordinates) on the elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$ and some positive integer k, we

compute kP.

1. Let $l = [x_m, x_{m-1}, \ldots, x_1]$ be the binary expansion of k so that $x_m \neq 0$.
2. Set $Q \leftarrow (0, 1, 0)$ and $R \leftarrow (x, y, z)$.
3. For $i = 1$ to m, if $x_i = 1$ set $Q \leftarrow Q + R$ and set $R \leftarrow R + R$. If $x_i \neq 1$ set $R \leftarrow R + R$.
4. Return Q.

With out elliptic curve group operations now established, we can begin our implementation of the Shanks-Mestre algorithm. The first thing we'll need is code to find the intersection of two sets. This will be used during the Shanks-Mestre Algorithm. We use the following algorithm from Crandall and Pomerance (see [5, Algorithm 7.5.1]).

Intersection: Given two finite sets $A = \{a_0, a_1, \ldots, a_{m-1}\}$ and $B = \{b_0, b_1, \ldots, b_{n-1}\}$ we return the intersection $A \cap B$.

1. Sort sets A and B in nondecreasing order. Set $i \leftarrow 0$, $j \leftarrow 0$ and let S be an empty set.
2. While $i < \#A$ and $j < \#B$
   (a) if $a_i \leq b_j$ append a_i to S if $a_i = b_j$. Then increment i until either $i > \#A - 1$ or $a_i \neq a_{i-1}$.
   (b) if $a_i \geq b_j$ increment j until either $j > \#B - 1$ or $b_j \neq b_{j-1}$.
3. Return S.

This intersection algorithm will be used in conjunction with the Baby-Step Giant-Step method in our Shanks-Mestre algorithm, which, once again, we adopt from Crandall and

Pomerance (see [5, Algorithm 7.5.3]).

Shanks-Mestre Algorithm: Given an elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$, we compute a_p.

1. If $p \leq 229$ use the Legendre algorithm to compute a_p.
2. Find a quadratic residue g modulo p.
3. Set $W \leftarrow \lceil p^{1/4}\sqrt{2} \rceil$, $c \leftarrow g^2 a$, and $d \leftarrow g^3 b$. [c and d are the twist parameters]
4. Choose a random integer x in $[0, p-1]$. Let $\sigma = (\frac{x^3+ax+b}{p})$. If $\sigma = 0$ choose new x. If $\sigma = 1$ set $E \leftarrow E_{A,B}$. If $\sigma = -1$ set $E \leftarrow E_{c,d}$ and $x \leftarrow gx$.
5. Find point $P = (x_1, y_1, z_1)$ on E so that $x_1 = x$.
6. Let $S \leftarrow shanks(P, E)$ [see below]. If the cardinality of S does not equal 1, return to Step 3.
7. Let $s \in S$. Let β be the index of s in A (from *shanks*). Let γ be the index of s in B (from *shanks*).
8. Choose sign in $t = \beta \pm \gamma W$ so that the point $(p + 1 + t)P$ is the identity on E.
9. Return $-1 \cdot \sigma \cdot t$.

Shanks: Given point P on elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$.

1. Let A and B be empty sets.
2. For $\beta = 0$ to $W - 1$, compute the point $(p+1+\beta)P$ on E and append the x-coordinate to A.
3. For $\gamma = 0$ to W, compute the point $(\gamma W)P$ on E and append the x-coordinate to B.
4. Return $A \cap B$.

Chapter 4

Further Considerations

Questions abound in analyzing champion primes. As we conclude our work, we illustrate some of the particularly interesting questions posed by our work and provide a collection of experimental data obtained using the open source software package GP (see [11]).

We began our work by considering the distribution of the primes, and the work leading up to the Prime Number Theorem. Similar questions can be asked concerning champion primes. That is, suppose we fix an elliptic curve $E_{A,B}$ and let $p \geq 5$ tend toward infinity. Does $E_{A,B}$ have any champion primes? If so, does $E_{A,B}$ have an infinite number of champion primes? We make the following definition.

Definition 14. Let $\pi_{A,B}(x) = \#\{4 < p < x \, : \, a_p(E_{A,B}) = -\lfloor 2\sqrt{p} \rfloor\}$.

We can then ask the following question.

- **Question 1**: Is there an asymptotic relationship for $\pi_{A,B}(X)$?

Some sample data is produced below.

(A, B)	$\pi_{A,B}(2^{31})$	Champion Primes
(1,1)	13	163, 1627, 9887, 80779, 35424097, 37962641, 52576253, 99328157, 125591327, 220697003, 251158981, 312060649, 445260407
(1,2)	9	3623, 624787, 5291647, 6362771, 7547017, 21311599, 31215497, 1006610929, 1548677453
(1,3)	16	11, 149, 991, 3709, 4217, 323083, 5622473, 13148407, 14465837, 20541043, 170750368, 186770131, 322163351, 555590689, 842815679, 959847211
(1,4)	12	29879, 1426627, 1450507, 4528219, 15228827, 21426049, 25325647, 32446919, 137462287, 224762833, 351781813, 1135278107
(1,5)	11	49639, 626929, 4758893, 8490637, 46088501, 58789463, 412208689, 479220857, 596160919, 981631043,1148278147
(1,6)	14	79, 10559, 12589, 26731, 55897, 137483, 5850791, 17571959, 114311381, 116543261, 277386089, 665162053, 975382559, 1443788299
(1,7)	8	1657, 31477, 385901, 209472209, 247435469, 357394649, 415849927, 1806444943
(1,8)	9	89, 624649, 1160813, 4568419, 26961607, 41888827, 186734279, 369055319, 1443410861
(1,9)	13	71, 271, 7489, 78101, 1908251, 9835951, 21578597, 29554667, 32402039, 47116309, 300411773, 587891503, 829370459,
(1,10)	5	5064739, 13056763, 65612563, 69995071, 89575951

Table 4.1: Counting Champion Primes

We next discussed Dirichlet's famous theorem concerning arithmetic progressions. Similar questions can be recast in the realm of champion primes for elliptic curves.

- **Question 2**: Given a fixed elliptic curve $E_{a,b}$, does there exist an infinite number of champion primes congruent to m modulo n.

We next recall that in Section 3.1.2 above we let A and B vary in search for a curve which had a specific prime p as a champion prime. A more intriguing question can be posed if we reverse these roles. That is, suppose we now fix integers A and B and let p vary until we find a champion prime on the elliptic curve $E_{A,B}$. One may then ask when the first champion prime will occur.

Definition 15. Let $F_{A,B}$ denote the first prime $p > 4$ that is a champion prime for $E_{A,B}$.

A sampling of data is reproduced below.

(A,B)	$F_{A,B}$	(A,B)	$F_{A,B}$	(A,B)	$F_{A,B}$	(A,B)	$F_{A,B}$	(A,B)	$F_{A,B}$
		(0,1)	67	(0,2)	97	(0,3)	7	(0,4)	13
(1,0)	53	(1,1)	163	(1,2)	3623	(1,3)	11	(1,4)	29879
(2,0)	37	(2,1)	664679	(2,2)	151537	(2,3)	71	(2,4)	41
(3,0)	5	(3,1)	11	(3,2)	729787	(3,3)	2647	(3,4)	131
(4,0)	29	(4,1)	71	(4,2)	1039	(4,3)	117017141	(4,4)	69737
(5,0)	17	(5,1)	151	(5,2)	41	(5,3)	1381	(5,4)	115499
(6,0)	29	(6,1)	3719	(6,2)	45757	(6,3)	18043	(6,4)	235813
(7,0)	257	(7,1)	419	(7,2)	1049	(7,3)	7	(7,4)	128599
(8,0)	5	(8,1)	59	(8,2)	29	(8,3)	1353499	(8,4)	89
(9,0)	29	(9,1)	151	(9,2)	1858579	(9,3)	3389	(9,4)	11
(10,0)	53	(10,1)	300967	(10,2)	47501	(10,3)	12619	(10,4)	4649
(11,0)	109	(11,1)	4083619	(11,2)	605893	(11,3)	389	(11,4)	53
(12,0)	17	(12,1)	16693	(12,2)	1931	(12,3)	11	(12,4)	821
(13,0)	5	(13,1)	419	(13,2)	1019	(13,3)	486341	(13,4)	13
(14,0)	17	(14,1)	11	(14,2)	266491	(14,3)	7	(14,4)	3517
(15,0)	37	(15,1)	137	(15,2)	5923	(15,3)	819853	(15,4)	270619
(16,0)	53	(16,1)	461	(16,2)	331	(16,3)	40099	(16,4)	1249
(17,0)	229	(17,1)	13633	(17,2)	239	(17,3)	331	(17,4)	359
(18,0)	5	(18,1)	181	(18,2)	17027	(18,3)	199	(18,4)	59
(19,0)	109	(19,1)	58991	(19,2)	71	(19,3)	50359	(19,4)	1587743
(20,0)	17	(20,1)	103	(20,2)	61469	(20,3)	587	(20,4)	11

Table 4.2: First Champion Primes

As you can see, the number of primes we have to consider before finding a champion prime varies greatly depending on the curve. Thus, one might ask the following questions.

- **Question 3**: Does there exist some constant C so that any given elliptic curve $E_{a,b}$ will have a champion prime less than C?
- **Question 4**: More generally, given an elliptic $E_{a,b}$, when does the first champion prime congruent to m modulo n occur?

Each of these questions, and many more, would be suitable for further research.

Bibliography

[1] N. Calkin, B.Faulkner, K. James, M. King, and D. Penniston. Average frobenius distributions for elliptic curves over abelian extensions. *Acta Arith.*, to appear.

[2] H. Cohen. *A course in computational algebraic number theory*. Graduate texts in mathematics. Springer-Verlag, 1993.

[3] W.A. Coppel. *Number theory: an introduction to mathematics*. Number pt. 2 in Number Theory: An Introduction to Mathematics. Springer, 2006.

[4] D.A. Cox. *Primes of the Form X + Ny: Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. John Wiley & Sons, 2011.

[5] R.E. Crandall and C. Pomerance. *Prime numbers: a computational perspective*. Lecture notes in statistics. Springer, 2005.

[6] J. Derbyshire. *Prime obsession: Bernhard Riemann and the greatest unsolved problem in mathematics*. Joseph Henry Press, 2003.

[7] M.J. Erickson and A. Vazzana. *Introduction to number theory*. Discrete mathematics and its applications. Chapman & Hall/CRC, 2008.

[8] M.R. Murty. *Problems in analytic number theory*. Graduate texts in mathematics. Springer, 2008.

[9] J.H. Silverman. *The arithmetic of elliptic curves*. Graduate texts in mathematics. Springer-Verlag, 1986.

[10] J.H. Silverman and J.T. Tate. *Rational points on elliptic curves*. Undergraduate texts in mathematics. Springer-Verlag, 1992.

[11] The PARI Group, Bordeaux. *PARI/GP, version* `2.5.0`, 2011. available from `http://pari.math.u-bordeaux.fr/`.